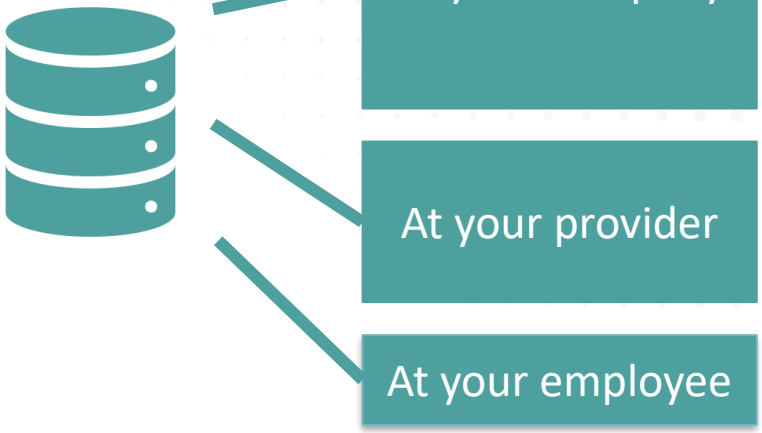
VISCHER

Being a Victim of a Cyber-Attack.

The Legal Side

David Rosenthal, Partner, VISCHER Ltd.
September 27, 2022

#1 Avoid data that can be stolen



- Data protection law **requires** storage limitation, i.e. only keep for as long as there is valid reason
- Have policies that require deletion and that avoid shadow copies and loose files; automate deletion
- You do not want to explain why data was stolen that should have been deleted long ago …

- You are legally **responsible** for your "processors"
- Think also of data left-over from old projects
- Have contracts be clear on this topic

- Prohibit your employees storing company data on their own private IT infrastructure

#2 Prepare from a legal point of view

- Know for each entity **when** and **where** to **report** a data breach and **how** (e.g., language, information and ID requirements)
- Have a data breach **notification policy**, including determining which responsibilities are local and which are central
- Make sure that each data breach is analyzed (standardized or individually) and **documented** even if not notified
- Have **emergency** contacts ready and outside counsel retained
- Have your data mapping available offline and have lists of those names, projects etc. that relate to **particularly critical data**
- Consider the risk of you being a victim when drafting **contracts**
- Do a **"DPIA"** before introducing an **"EDR"** and similar tool

Also consider cross-border notifications

Expect your service providers to report data breaches, too

Also with a view to legal privilege

penalties, audit clauses, reporting obligations, force majeure events

#3 Report and follow the 80:20 rule

- The key question: **Which data**, if any, did they get?
  - Focus on really critical data, consider monitoring the Darknet
  - Consider performing a review, but follow the 80:20 rule
- **Regulators** – remain vague, show that all is under control
  - Do not report theoretical risks, but document risk assessment
  - Keep in mind the short notification periods (GDPR: 72 hours)
- **Employees, customers, partners** – show fast that you care
  - Don't report too much publicly, tell what you do and they can do
  - Not only personal data is at issue, but also third-party secrets
- **Shall we call the police?** It may have various advantages …

Contracts may also require you to inform or even permit audits; being forthcoming prevents nasty questions

#4 Consider paying ransom

- Paying ransom can be a valid **business decision**
  - The police will advise against, it may expose you to follow-up attacks, but you may protect customers and be able to negotiate
  - Try to understand your opponent (e.g., is triple extortion likely?)
  - 46% pay and get back data, but almost nobody gets back all*
- Paying ransom is in our view **permitted** under Swiss law
  - Art. 260ter SPC – financial support of a criminal organization?
  - Making a payment may be difficult (sanctions, AML measures)
- Ransomware payments are in our view **tax-deductible**
  - As are proven damages that occurred due to a cyberattack

https://www.nomoreransom.org

* Source: https://www.sophos.com/de-de/whitepaper/state-of-ransomware

#5 Handle the consequences

- **Costs** of handling data breach cases are increasing quickly
- **Regulatory** and criminal **investigations** against the victim
  - Fines for inadequate data security (triggered by notifications, complaints or whistleblowing reports)
- Lawsuits by **customers, partners** and others
  - Not yet prevalent here, but on the rise in certain countries (e.g., in the US, Germany and the UK)
  - Here, most customers and partners are still forgiving
- Sue your own **your own provider**?
  - For lack of adequate data security measures
  - But: Indirect and consequential damages are difficult to prove

Key Take-Aways

- Have your organization **delete** any data no longer needed, because what is gone cannot be stolen and disclosed anymore
- Know the data breach **notification rules** for each jurisdiction in which you do relevant business (can you cope with them on short notice?) and have **data breach notification policy**
- If data has been stolen, **focus** on the critical data and try to identify it, but do not worry if you miss out some – draw the line based on the 80/20 rule and **document** your decisions
- Data breaches can expensive and expose customers; therefore, whether to pay ransom should also be a **business decision**
- For most data breaches we got involved in, business returned back to normal **within 6-12 months**

Source: heimdalsecurity.com

VISCHER

Thank you for your attention!

Questions: drosenthal@vischer.com

Zürich
Schützengasse 1
Postfach
8021 Zürich, Schweiz
T +41 58 211 34 00

Basel
Aeschenvorstadt 4
Postfach
4010 Basel, Schweiz
T +41 58 211 33 00

Genf
Rue du Cloître 2-4
Postfach
1211 Genf 3, Schweiz
T +41 58 211 35 00

www.vischer.com